CLAIMS

1. A method for protecting electronic files, comprising:

obtaining environment information regarding a computer, the environment information including data concerning an operating environment of the computer;

generating an encryption key based on the environment information; and

encrypting an electronic file using the encryption key.

2. A method as recited in claim 1, further comprising the operation of creating a decryption key based on environment information, wherein the decryption key can be utilized to decrypt the electronic file.

3. A method as recited in claim 2, wherein the encryption key and the decryption key are public key infrastructure (PKI) based keys.

4. A method as recited in claim 1, wherein the environment information includes location information of the computer.

5. A method as recited in claim 4, wherein the location information specifies a location of the computer within a predetermined range.

6. A method as recited in claim 5, wherein the location information is provided by global positioning satellite (GPS) data.

7. A method as recited in claim 1, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored.

8. A method as recited in claim 7, wherein the drive information includes a drive identifier that identifies the particular drive wherein the electronic file will be stored.

9. A method as recited in claim 7, wherein the drive information includes an electronic address assignment of the particular drive wherein the electronic file will be stored.

10. A method as recited in claim 1, wherein the environment information includes time information specifying access duration.

11. A method as recited in claim 10, wherein the access duration is a time range indicating a time period when the electronic file can be accessed.

12. A method as recited in claim 11, wherein the electronic file cannot be decrypted at a time outside the time range.

13. A method as recited in claim 10, wherein the access duration is a date range indicating a range of dates when the electronic file can be accessed.

14. A method as recited in claim 13, wherein the electronic file cannot be decrypted at a date outside the date range.

15. A method for protecting electronic files, comprising:

storing an electronic file encrypted using an encryption key, wherein the encryption key is generated using a first environment profile of a computer, and wherein the environment profile includes data concerning an operating environment of the computer;

obtaining a second environment profile of the computer based on a current operating environment of the computer;

generating a decryption key based on the second environment profile; and

decrypting the electronic file using the decryption key.

16. A method as recited in claim 15, wherein the encryption key and the decryption key are further based on a passcode received from a user.

17. A method as recited in claim 16, further comprising the operation of appending the first environment profile to the passcode to generate the encryption key.

18. A method as recited in claim 17, further comprising the operation of appending the current environment profile to the passcode to generate the decryption key.

19. A method as recited in claim 18, wherein the decryption key cannot decrypt the electronic file when the current environment profile does not match the first environment profile.

20. A method as recited in claim 19, wherein a match occurs when the data in the current environment profile is within a predetermined range of the data in the first environment profile.

21. A method as recited in claim 15, wherein the environment profile includes location information specifying a location of the computer within a predetermined range.

22. A method as recited in claim 21, wherein the location information is provided by global positioning satellite (GPS) data.

23. A method as recited in claim 15, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored.

24. A method as recited in claim 15, wherein the environment information includes time information specifying access duration, wherein the access duration is a time range indicating a time period when the electronic file can be accessed.

25. A method as recited in claim 15, wherein the environment information includes date information specifying access duration, wherein the access duration is a date range indicating dates that the electronic file can be accessed.

26. A method for protecting electronic files, comprising:

authenticating a digital transaction using a delay number based on a timing signal received from a remote source;

obtaining environment information regarding a computer, the environment information including data concerning an operating environment of the computer;

generating an encryption key based on the environment information; and

encrypting an electronic file using the encryption key.

27. A method as recited in claim 26, wherein the delay number is based on a delay time period between when the timing signal was transmitted and when the timing signal was received.

28. A method as recited in claim 27, wherein the delay in the timing signal is caused by free electrons in a line of sight between the remote source and a receiver.

29. A method as recited in claim 28, wherein the delay in the timing signal is further caused by variations in atmospheric conditions.

30. A method as recited in claim 26, further comprising the operation of creating a decryption key based on environment information, wherein the decryption key can be utilized to decrypt the electronic file.

31. A method as recited in claim 30, wherein the encryption key and the decryption key are public key infrastructure (PKI) based keys.

32. A method as recited in claim 26, wherein the environment information includes location information specifying a location of the computer within a predetermined range.

33. A method as recited in claim 32, wherein the location information is provided by global positioning satellite (GPS) data.

34. A method as recited in claim 26, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored.

35. A method as recited in claim 26, wherein the environment information includes time information specifying access duration, wherein the access duration is a time range indicating a time period when the electronic file can be accessed.

36. A method as recited in claim 35, wherein the electronic file cannot be decrypted at a time outside the time range.

37. A method as recited in claim 26, wherein the environment information includes date information specifying access duration, wherein the access duration is a date range indicating dates that the electronic file can be accessed.

38. A method as recited in claim 37, wherein the electronic file cannot be decrypted on a date outside the date range.